Team TSI Application Service Provider Privacy & Security Policies

Access	TSI shall use commercially reasonable efforts to provide the Software Services on a 24/7 basis with prior notice provided for routine, scheduled maintenance. Access to the application is provided over a 128 bit SSL connection.
Authorization	Authorization of users is determined by each customer. Unique user accounts are created by either the customer or by TSI at the customer's direction. Authorization can be revoked by disabling any user account with the Portal's user administration utility.
Authentication	Users are authenticated by the Portal through the use of a password and Company ID combination. TSI also supports a "token pass" authorization system where the customer authenticates the user and passes a token to TSI. TSI uses this token to dynamically set user authorization, roles and other portal access rights. The Portal can monitor who is using the various sections of the Portal and from what IP address the Portal is being accessed from.
Audit	TSI periodically reviews policies and procedures in reference to firewall security, application security, infrastructure and physical access to the data center. Any discrepancies are corrected and tested for compliance.
Secondary Uses of Data	We do not release or use any ePHI data for releases to outside sources, nor do we use it for peer group analysis without client release, we do however use our public data sources for many types of secondary uses and analysis.
Data Ownership	TSI acknowledges and agrees that the data and information that is compiled or passes through the databases that are a part of the Software Services and that specifically relates to patients, patient care or physician procedures or diagnosis (collectively, the "Customer Data"), and all right, title and interest therein, is and shall remain the exclusive property of Customer.